Report Configurazione Laboratorio SIEM con Wazuh

Josh Van Edward Abanico

4 febbraio 2026

Indice

1 Architettura e Topologia di Rete **3**

2 Installazione e Configurazione dell'Agente Wazuh **3**
2.1 Installazione del Pacchetto 3
2.2 Configurazione dell'Enrollment 3

3 Test di Funzionalità e Rilevamento Minacce **4**
3.1 Scenario di Test: Accesso SSH 4
3.2 Analisi degli Alert sulla Dashboard 5

1 Architettura e Topologia di Rete

L'infrastruttura di laboratorio è stata progettata su un segmento di rete isolato (subnet `192.168.50.0/24`), gestito tramite firewall pfSense per garantire il routing e la sicurezza perimetrale.

La topologia prevede tre nodi principali configurati con i seguenti indirizzi IP statici:

- **Gateway / Firewall (pfSense):**
  - **IP:** `192.168.50.1`
  - **Ruolo:** Gestione del routing, server DHCP e punto di accesso alla rete esterna.
- **SIEM Server (Wazuh Manager):**
  - **IP:** `192.168.50.13`
  - **Installazione:** Virtual Appliance (OVA) importata su VirtualBox.
  - **Ruolo:** Centralizzazione dei log, analisi degli eventi di sicurezza e dashboard di visualizzazione.
- **Endpoint / Agente (Kali Linux):**
  - **IP:** `192.168.50.100` (Configurazione statica)
  - **Ruolo:** Macchina target utilizzata per la simulazione di attacchi e il monitoraggio degli eventi di sicurezza.

2 Installazione e Configurazione dell'Agente Wazuh

Per abilitare il monitoraggio sull'endpoint Kali Linux, è stato installato il pacchetto `wazuh-agent` seguendo la documentazione ufficiale del produttore.

2.1 Installazione del Pacchetto

L'installazione su Kali Linux (distribuzione basata su Debian) è stata eseguita aggiungendo la chiave GPG del repository ufficiale e installando il pacchetto tramite `apt`.
Riferimento utilizzato: Wazuh Agent Package - Linux Documentation

2.2 Configurazione dell'Enrollment

L'agente è stato collegato al Manager modificando manualmente il file di configurazione locale, invece di utilizzare i comandi di registrazione automatica via password o API.

La procedura seguita è stata la seguente:

1. Modifica del file di configurazione principale situato in `/var/ossec/etc/ossec.conf` sulla macchina Kali Linux.

2. All'interno del blocco `<client><server><address>`, è stato specificato l'indirizzo IP del server Wazuh (`192.168.50.13`).
3. Abilitazione e avvio del servizio tramite `systemctl`.

```
# Ricarica dei demoni e avvio del servizio Wazuh
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Listing 1: Comandi per l'avvio dell'agente

Riferimento utilizzato: Enrollment via Agent Configuration

3 Test di Funzionalità e Rilevamento Minacce

Per verificare la corretta comunicazione tra l'agente Kali (`192.168.50.100`) e il server Wazuh (`192.168.50.13`), è stato eseguito uno scenario di test basato sull'accesso remoto.

3.1 Scenario di Test: Accesso SSH

È stata avviata una sessione SSH verso la macchina Kali Linux con l'obiettivo di generare eventi di autenticazione nei log di sistema (specificamente in `/var/log/auth.log`).

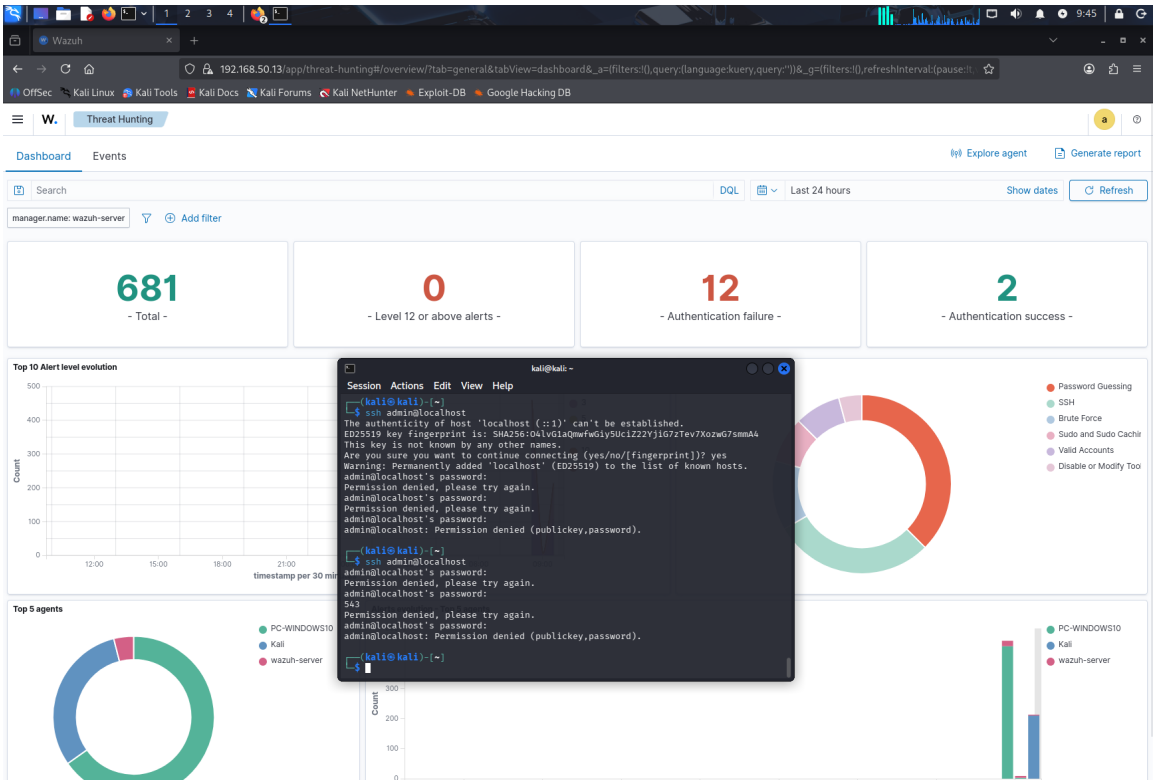

Figura 1: Tentativo di accesso SSH, alert in sottofondo.

3.2 Analisi degli Alert sulla Dashboard

Accedendo alla Dashboard web di Wazuh (`https://192.168.50.13`), sono stati riscontrati i seguenti risultati:

1. Lo stato dell'agente Kali Linux risulta correttamente su **Active**.
2. Nel modulo **Security Events**, il sistema ha rilevato e indicizzato in tempo reale gli eventi relativi alla connessione SSH effettuata.

Conclusione del Test: Il sistema ha dimostrato la capacità di ricevere i log dalla rete `192.168.50.x`, decodificarli correttamente tramite le regole standard e visualizzarli sulla dashboard, confermando la piena operatività dell'architettura SIEM implementata.